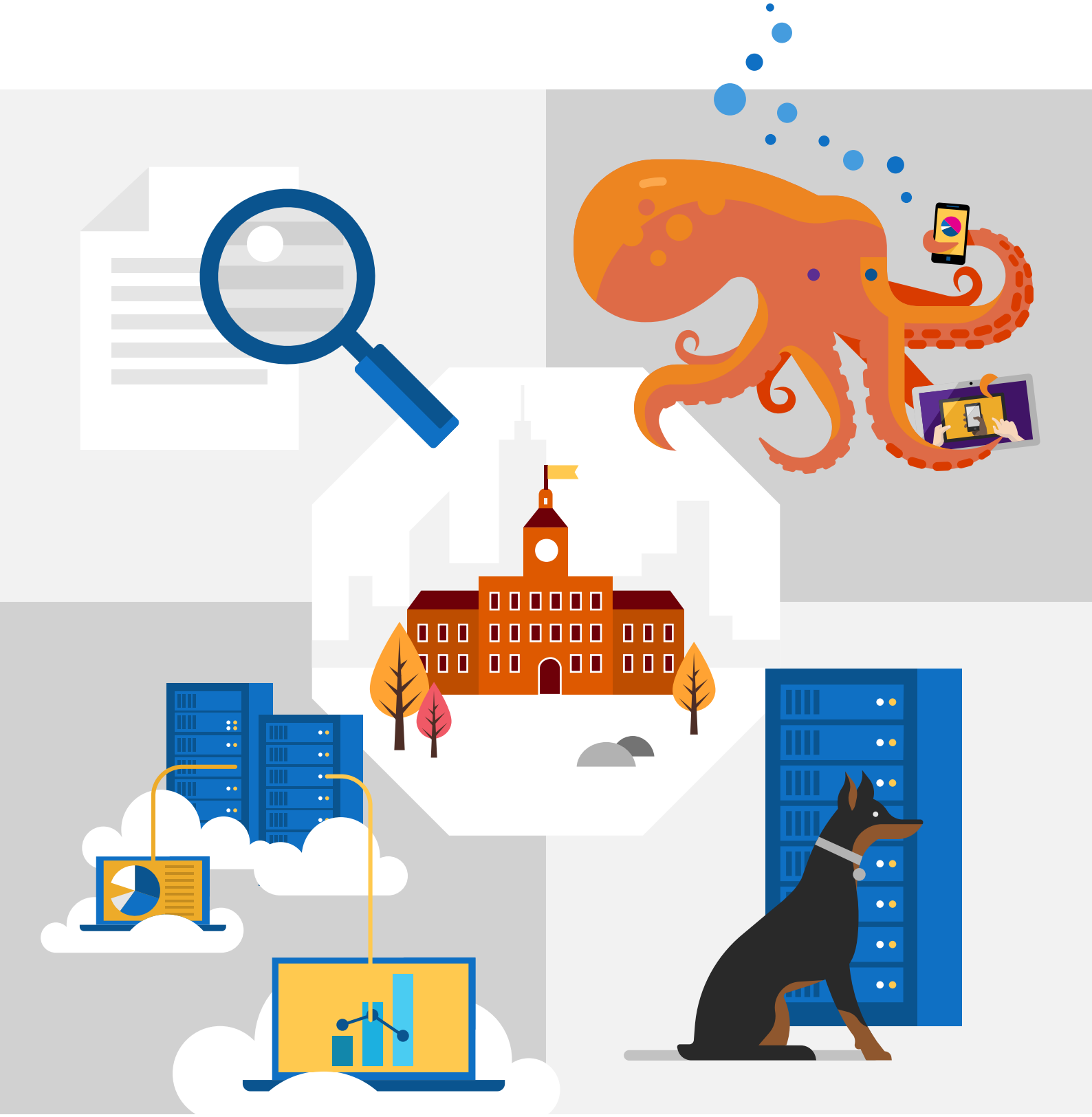


Die GDPR im Bildungssektor

Erste Schritte – ein Leitfaden für Bildungseinrichtungen

Microsoft

Über diesen Leitfaden

Dieser Leitfaden wurde dazu ausgearbeitet, Ihnen durch konkrete Beispiele und To-Do-Listen bei der Einhaltung der Datenschutz-Grundverordnung GDPR (General Data Protection Regulation) zu helfen. Er bietet zwar keine abschliessende Information, wird Ihnen jedoch eine gute Vorstellung von den Verfahren und Faktoren geben, die nach dem Inkrafttreten der GDPR am 25. Mai 2018 beachtet werden müssen.

Die GDPR gilt für alle Institutionen, die eine Niederlassung in der EU haben, sowie für Organisationen, die EU-Bürgern Waren und Dienstleistungen anbieten, oder die personenbezogene Daten von EU-Bürgern erfassen und analysieren.Wenn Ihre Institution ausserhalb der EU angesiedelt ist, sollten Sie diesen Leitfaden zur GDPR-Compliance als einen Best-Practice-Ansatz betrachten.

Bildung ist eine Daten-Story

Zum Beginn eines jeden Schul- bzw. Studienjahres sorgen neue Schüler und Studenten in Schulen und Universitäten für gewaltige Datenmengen. Hierdurch wachsen die Datenberge, die diese Organisationen als Dateneigentümer bereits handhaben, ständig weiter an.

Doch diese Daten sind unverzichtbar für das reibungslose Funktionieren der Schulen und Unis. Deshalb müssen für jeden verarbeiteten Datensatz klare, gut dokumentierte Verfahren bestehen.

Darüber hinaus müssen diese Verfahren mehr als nur die Zeit abdecken, die die Schüler/Studenten bei Ihnen verbringen. Auch nachdem diese Ihre Bildungseinrichtung verlassen haben, sind weiterhin dokumentierte Richtlinien zu Schutz, Aufbewahrung und Verarbeitung von Datenbanken, Dateien, ja selbst E-Mail-Kommunikationen erforderlich.

Definierung des Datenweges

Die von Bildungseinrichtungen erstellten und verarbeiteten Informationen dienen vielen verschiedenen Zwecken.

Zunächst ist da der Lehrplan: das Wissen, das die Lehrenden den Lernenden vermitteln, und das die Schüler/Studenten im Laufe ihres Lernweges durch eigene Ideen bereichern.

Daneben gibt es noch eine zweite Gruppe von Daten: die Informationen, die Organisationen über die Lehrenden, Lernenden und die Leistung der Bildungseinrichtung erfassen. Hinzu kommen Informationen, die bei Verwaltungsabläufen gesammelt werden – von Eltern, medizinischem Personal, Eltern-/Kommunalvertretern und externen Stellen. So durchfliesst ein nie enden wollender Strom von Daten die Organisation, wobei ein grosser Teil davon personenbezogene Daten sind.

Wie jeder Verwalter weiss, sind die Daten der zweiten Art nicht weniger wichtig für den Bildungsauftrag von Bildungseinrichtungen. Sie bilden einen wesentlichen Bestandteil der GDPR-Prozesse, denen Schüler/Studenten, Lehrkräfte und Eltern begegnen, während sie durch die von Schulen und Unis bereitgestellten Lernmittel und Kommunikationsdienste auf Informationen zugreifen und diese miteinander austauschen.

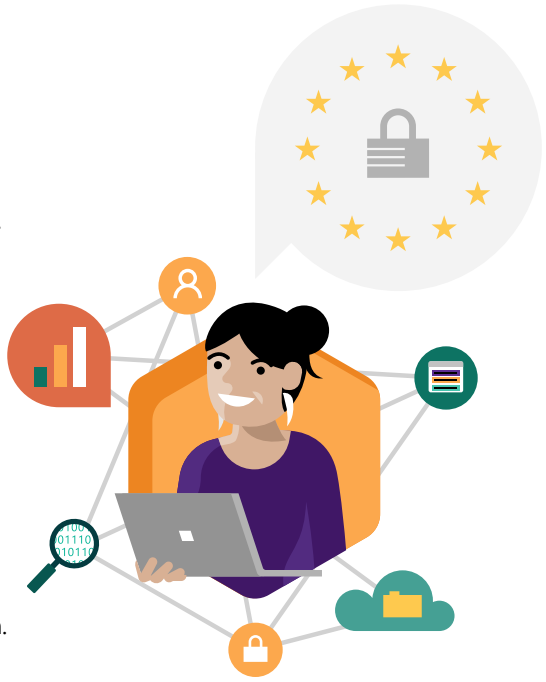
Was soll mit all diesen Daten geschehen?

Als Dateneigentümer unterliegen Sie bereits bestehenden Gesetzen, die die sorgsame Handhabung und Verarbeitung aller Daten, die Sie besitzen und verarbeiten, vorschreiben. Die GDPR verlangt nun zusätzliche Überlegungen dazu, wie, warum und mit wem (z. B. Regulierungsbehörden, staatlichen Stellen und ggf. anderen Dritten, wie Versicherungsunternehmen) Sie gewisse Daten teilen und wie Sie sie verarbeiten und analysieren. Dabei besitzen Sie wahrscheinlich ohnehin schon zahlreiche Richtlinien zum Schutz der Daten und Privatsphäre.

Aber reichen diese aus, die personenbezogenen und sensiblen Daten zu schützen, mit denen Sie umgehen?

Einführung in die GDPR

Gemäss der neuen EU-Datenschutz-Grundverordnung (GDPR), werden ab dem 25. Mai 2018 viele Organisation – selbst solche, die sich ausserhalb der Europäischen Union befinden – der Rechenschaftspflicht für alle ihre Daten unterliegen.
Das Ziel der Verordnung ist, die personenbezogenen Daten aller EU-Bürger zu schützen und die Datenschutzgesetze in ganz Europa zu harmonisieren. Die GDPR hat Auswirkungen darauf, welche Daten Sie haben, wie sie genutzt und wo sie gespeichert werden, und wie lange sie gespeichert werden dürfen.



Warum ist die GDPR wichtig?

Der Weg einer Bildungseinrichtung kann den Lernweg ihrer Schüler/Studenten wiederspiegeln – markiert von Meilensteinen, die in jedem Stadium festgehalten und bewertet werden. Manchmal bleiben die generierten Daten jahrelang dieselben, manchmal ändern sie sich schnell, während die Schüler/Studenten und Lehrkräfte die Einrichtung durchlaufen.

Die GDPR schafft einen einheitlichen EU-Rechtsrahmen und gibt allen in Europa wohnhaften Bürgern Rechte an diesen Daten.

Zu den wichtigsten Änderungen für den Bildungsbereich gehören:

Privatsphäre

Einzelpersonen haben das Recht:

- Auf ihre personenbezogenen Daten zuzugreifen
- Fehler in ihren personenbezogenen Daten zu berichtigen
- Ihre personenbezogenen Daten zu löschen
- Der Verarbeitung ihrer personenbezogenen Daten zu widersprechen
- Ihre eigenen personenbezogenen Daten zu exportieren

Kontrollen und Benachrich-tigungen

Von Ihnen wird verlangt, dass Sie:

- Personenbezogene Daten durch angemessene Sicherheitsmassnahmen schützen
- Die Aufsichtsbehörden über Verletzungen des Schutzes personenbezogener Daten unterrichten
- Dokumentieren, wie Sie personenbezogene Daten verarbeiten
- Aufzeichnungen über Datenverarbeitung und Einwilligungen verwahren*

Transparente Richtlinien

Von Ihnen wird erwartet, dass Sie:

- Datenerfassungen klar ankündigen
- Den Zweck der Datenverarbeitung und -nutzung klar umreissen
- Richtlinien zur Datenaufbewahrung und -löschung festlegen
- Umreissen, wie Kunden die Rechte wahrnehmen können, die ihnen aus der GDPR erwachsen

IT und Training

Von Bildungseinrichtungen wird verlangt, dass sie:

- Mitarbeiter im Datenschutz schulen – z. B. Verwaltungsmitarbeiter der Schule oder IT-Personal
- Richtlinien prüfen und aktualisieren, die sich auf Schüler/Studenten, Lehrkräfte und Auftragnehmer beziehen
- Einen Datenschutzbeauftragten ernennen (falls erforderlich)
- Für alle Anbieter, inkl. Vertretungslehrkräfte, konforme Anbieter-Verträge erstellen und verwalten

***Die GDPR enthält besondere Schutzregeln für Kinder. Sie schreibt vor, dass die Einwilligung von Kindern „ausdrücklich" erfolgen muss. Die GDPR legt die Einwilligungsfähigkeit im Online-Bereich auf 16 Jahre fest. Den EU-Mitgliedstaaten steht es jedoch frei, eine eigene Grenze zwischen 13 und 16 Jahren zu setzen.**

Inwiefern betrifft Sie die GDPR?

Wie können Sie diese neuen Vorschriften mit der Tatsache in Einklang bringen, dass zahlreiche Personen in Ihrer Organisation tagtäglichen Zugriff auf Daten haben müssen?

Die GDPR liefert Bestimmungen zu Verwaltung und Schutz dieser Daten, indem sie einheitliche Richtlinien und Verfahren breitstellt. Es liegt nun ganz bei Ihnen, einen GDPR-Rahmen zu schaffen, der den Bedürfnissen Ihrer Organisation entspricht.

Verbesserte Datenschutzrechte

Die GDPR verstärkt den Datenschutz für Einzelpersonen, inkl. Schülern/Studenten, innerhalb der EU, indem sie ihnen folgende Rechte sichert:

- Recht auf Datenzugriff und -berichtigung
- Recht auf Löschung
- Recht auf Widerspruch gegen Verarbeitung ihrer Daten
- Recht auf Datenübertragung

Erhöhte Verpflichtung, Verfahren zu dokumentieren und Daten zu schützen

Bildungseinrichtungen, die personenbezogene Daten verarbeiten, müssen klare Compliance-Nachweise

Berichtspflicht bei Datenschutzverstössen

Bildungseinrichtungen müssen Datenschutzverstösse binnen 72 Stunden melden.

Erhebliche Strafen bei Nichteinhaltung

Wenn Bildungseinrichtungen nicht aktiv werden, riskieren sie Strafen. Um Konformität sicherzustellen, ist es notwendig, mehrere Massnahmen zum Schutz personenbezogener Daten in Betracht zu ziehen und umsichtig mit Daten umzugehen.

Wo sollten Sie anfangen? Hinweise zur Einhaltung der GDPR

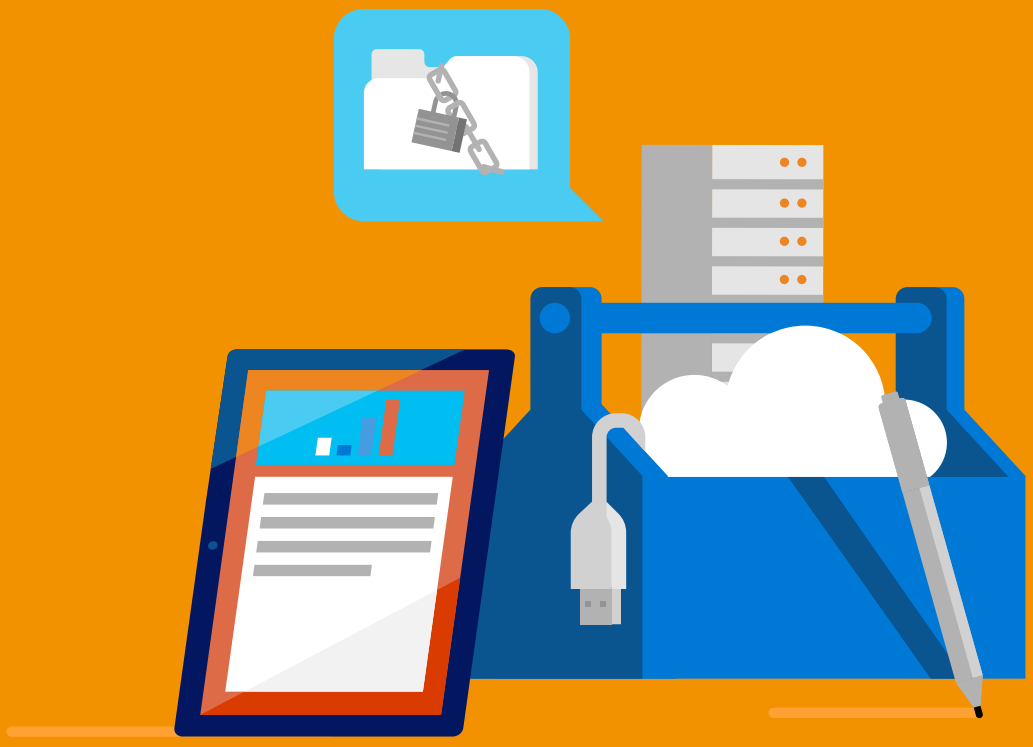
Die GDPR wird erhebliche Auswirkungen auf Ihre Bildungseinrichtung haben. Sie verlangt, dass Sie die Richtlinien für den Schutz personenbezogener Daten aktualisieren, Datenschutzmassnahmen und Verstossmeldeverfahren implementieren oder verstärken, sich höchst transparenter Verfahren bedienen und weiter in IT und Training investieren.

Als Anbieter von Clouddiensten mit dem umfangreichsten Compliance-Angebot können wir Ihnen mit der Microsoft Cloud den Weg zur GDPR-Compliance ebnen. Sie werden sehen, dass Ihnen die Microsoft Cloud die meisten Ressourcen an die Hand gibt, die Sie zur Erfüllung der GDPR-Bestimmungen benötigen.

Wir haben ein Verfahren zur GDPR-Implementierung entwickelt, dass sich auf vier Hauptschritte konzentriert:

- **Ermitteln.** Feststellen, welche personenbezogenen Daten bei Ihnen vorhanden sind und wo diese gespeichert sind
- **Verwalten.** Festlegen, wie personenbezogene Daten genutzt werden und wie auf sie zugegriffen wird
- **Schützen.** Einrichten von Kontrollen, um Schwachstellen und Datenschutzverstösse zu verhindern, zu erkennen und zu beheben
- **Berichten.** Archivieren nötiger Dokumentationen, Verwalten von Datenanfragen und Benachrichtigen über Datenschutzverstösse

Microsofts Tools und Ressourcen können Ihnen in jedem Stadium dabei helfen, GDPR-Compliance sicherzustellen.



Ermitteln

Verwalten

Berichten

Schützen

Ermitteln

Feststellen, welche personenbezogenen Daten bei Ihnen vorhanden sind und wo diese gespeichert sind.

Feststellen, was Sie haben

Personenbezogene Daten sind oft an mehreren Orten gespeichert, inkl. in E-Mails, Dokumenten, Databanken, Wechselmedien, Metadaten, Logdateien und Datensicherungen.

Zunächst gilt es zu ermitteln, wo personenbezogene Daten erfasst und gespeichert werden.

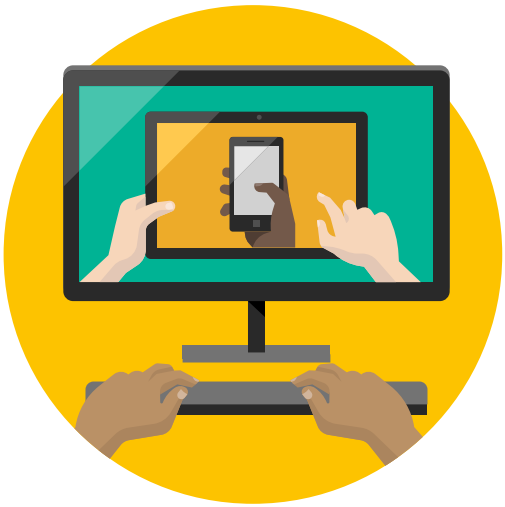
Vorhandene Daten

Herausforderung

Sie müssen die vorhandenen Daten nicht nur auf GDPR-konforme Weise aufbewahren und schützen, sondern auch dokumentieren, wie Sie personenbezogene Daten verarbeiten, z. B.: 1. Einwilligung, 2. Vertrag, 3. Recht, 4. Gesundheit, 5. gängiger Grund, 6. berechtigter Grund.

To-Dos

- Feststellen, welche personenbezogenen Daten erfasst und gespeichert sind.
- Ermitteln, an welchen Orten Daten gespeichert sind. Denken Sie bitte daran, Cloud-Anbieter und Hosting-Drittanbieter wie Websites und Shared Service Center mit zu berücksichtigen. Und vergessen Sie nicht die analogen Daten, die Sie in Ablageschränken aufbewahren.
- Vorhandene Daten nach Sensibilität, Nutzung, Eigentum, Administratoren und Nutzern ordnen und beschriften.
- GDPR-Gründe für die Verarbeitung dokumentieren.
- Das Einwilligungsverfahren prüfen und wenn nötig erneuern.



Bestehende Geräte und Standorte

Herausforderung

Personenbezogene Daten sind oft auf vielen verschiedenen Geräten gespeichert, die alle zum Zugriff auf sie genutzt werden können. Zu solchen Geräten gehören beispielsweise Server, Desktop-Computer, Laptops, Tablets, Smartphones und Heimrechner sowie gemanagte und nicht-gemanagte Cloud-Umgebungen. Persönliche und mobile Geräte stellen eine besondere Herausforderung dar, wenn es um die Ermittlung von Daten geht.

To-Dos

- Eine Bestandsaufnahme und Liste von allen Geräten machen, auf denen sich personenbezogene Daten befinden könnten.
- Alle persönlichen und mobilen Geräte überprüfen, die sich nicht im Besitz Ihrer Bildungseinrichtung befinden.

GDPR-Anforderungen

Die GDPR schreibt vor, dass Organisationen feststellen, welche Daten vorhanden sind und wo sie sich befinden.

Nachdem Sie eine Bestandsaufnahme aller Daten – inkl. Standorte, Geräte und Nutzer – gemacht haben, können Systeme zur Erfassung neu eingehender Daten eingerichtet werden.

Bestehende Nutzer

Herausforderung

Die GDPR stellt strenge Regeln dafür auf, wer welche personenbezogenen Daten verarbeiten darf, und wie und wann dies zulässig ist. Bevor Sie personenbezogene Daten mit anderen teilen, müssen Sie sicherstellen, dass alle, die innerhalb oder ausserhalb Ihrer Bildungseinrichtung auf sie zugreifen, zu ihrer Ansicht berechtigt sind.

To-Dos

- Alle Nutzer identifizieren und auflisten, einschliesslich aller Schüler/Studenten, Lehrkräfte und Auftragnehmer, die auf Daten zugreifen könnten.

Bestehende Auftragnehmer

Herausforderung

Personenbezogene Daten dürfen nur mit berechtigten Personen geteilt werden, und nur solche dürfen auf sie zugreifen. Das gilt sowohl für Personen innerhalb als auch ausserhalb Ihrer Organisation, also auch für alle Auftragnehmer, mit denen Ihre Einrichtung zusammenarbeitet, z. B. Catering- und Reinigungsdienste und andere externe Agenturen.

Es liegt in Ihrer Verantwortung sicherzustellen, dass die zum Datenzugriff berechtigten Personen (unter der GDPR „Auftragsverarbeiter" genannt) die gesetzlichen Vorschriften einhalten. Das heisst, dass sie die personenbezogenen Daten sicher speichern, sie nur für die von Ihnen genannten Zwecke verwenden und sie löschen, wenn sie nicht mehr benötigt werden.

To-Dos

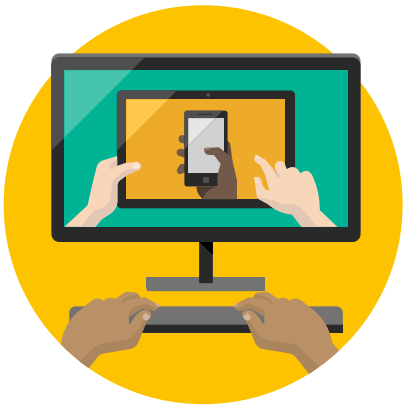
- Alle Auftragnehmer identifizieren und im Benutzerverzeichnis auflisten.
- Auf GDPR-Konformität überprüfen.
- Einen GDPR-Konformitätsvertrag unterzeichnen.
- Noch vor Ort nachprüfen, ob Daten zentral abrufbar sind.

Verwalten

Festlegen von Zugriff und Nutzung für personenbezogene Daten.

Personenbezogene Daten verwalten

Der erste Schritt zur Verwaltung personenbezogener Daten besteht darin festzustellen, wieso Sie sie überhaupt erfassen müssen. Fragen Sie sich, ob sie Ihnen bei der Bereitstellung Ihres Bildungsangebots helfen werden. Überlegen Sie, wie sie erfasst werden sollten, wo sie gespeichert werden, welche Stellen das Verfahren unterstützen werden, wer auf sie zugreifen sollte und wie Sie Änderungen und Löschungen ermöglichen werden.



Neue Daten verwalten

Herausforderung

Die GDPR erlaubt die Nutzung von Daten, die Sie für Ihren Auftrag benötigen. Wenn Ihr Auftrag klar definiert ist, wird die Notwendigkeit zur Verarbeitung von mit ihm verknüpften personenbezogenen Daten grösser sein.

Bei der Registrierung von Schülern/Studenten werden Sie transparent darüber sein wollen, welche Daten Sie erfassen. Insbesondere müssen Sie wissen, warum Sie diese Daten benötigen, wie lange Sie sie aufbewahren werden, wo Sie sie speichern und wie Sie und andere auf sie zugreifen werden.

Falls relevant, muss eine Einwilligung für die Datenverarbeitung angefordert, in Empfang genommen und zum Nachweis gespeichert werden.

Minderjährige Schüler/Studenten werden die Einwilligung ihrer Eltern benötigen. Wenn Sie Mitarbeiter einstellen, müssen Sie diese klar darüber informieren, wie personenbezogene Daten verarbeitet werden.

To-Dos

- Ihren Auftrag klar definieren.
- Ihre Datensubjekte auflisten.
- Feststellen, welche personenbezogenen Daten benötigt werden.
- Die Datenerfassung automatisieren und Prinzipien der Rechenschaftspflicht beachten.
- GDPR-Vertragsklauseln mit Ihrem HR-Partner abklären, Einwilligungen überprüfen und Verfahren, falls erforderlich, erneuern.

Geräte verwalten

Herausforderung

Im Bildungsumfeld existieren viele verschiedene Geräte, die von einem breiten Spektrum von Personen benutzt werden. Da gibt es die Heimcomputer von Lehrkräften, die Smartphones und Tablets von Schülern/Studenten, Klassenzimmer-Computer, persönliche Geräte, private Apps, nicht überwachte Cloud-Apps und -Standorte, Geräte von Unterauftragnehmern, USB-Schlüssel und in Schränken verwahrte Papierakten.

Um den strengen GDPR-Regeln zum Schutz personenbezogener Daten zu entsprechen, werden Sie alle Geräte – sowie alle Lehrkräfte, Schüler/Studenten und Auftragnehmer – auf konsequente Weise verwalten müssen.

To-Dos

- Richtlinien zur Nutzung von Geräten ausarbeiten.
- Lehrkräfte und Schüler/Studenten informieren und auf die GDPR hinweisen.
- Ereignisse überprüfen und protokollieren.

GDPR-Anforderungen

Die GDPR schreibt vor, wie personenbezogene Daten genutzt werden dürfen und wie der Zugriff auf sie zu regeln ist.

Nutzer verwalten

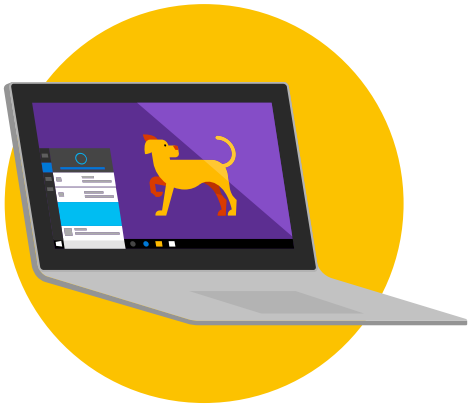
Herausforderung

Während Ihnen der Ermittlungsprozess Einblicke in Ihre Nutzerdatenbank gibt, hilft Ihnen der Verwaltungsprozess, die Nutzer in intelligente Listen zu sortieren, sodass Sie Berechtigungen setzen, Richtlinien zur sicheren Anmeldung aufstellen und den Zugriff verfolgen können.

Wenn Nutzer Ihre Bildungseinrichtung verlassen, muss ihr Zugriff auf alle Ihre Ressourcen so bald wie möglich unterbunden werden, um die Gefahr von Datenlecks weitgehendst zu begrenzen.

To-Dos

- Nutzer in Sicherheitsgruppen unterteilen.
- Berechtigungen und Richtlinien definieren.
- Richtlinien implementieren.
- Schüler/Studenten, Lehrkräfte und Auftragnehmer in korrekter Datenverwendung schulen.



Ihre Website verwalten

Herausforderung

Online-Aktivitäten sind ein wichtiger Bestandteil von Werbeaktionen zur Gewinnung von Schülern/Studenten. Sie sind verpflichtet, auf den von Ihnen verwendeten Online-Plattformen für Datensicherheit zu sorgen.

To-Dos

- Die von Ihrer Website erfassten Daten automatisch überprüfen.
- Cookies von Erst- und Drittanbietern auflisten.
- Online-Formulare auf End-to-End-Sicherheit prüfen.
- Einwilligungsverfahren auf GDPR-Konformität prüfen.
- Eine Datenschutzerklärung erstellen, die dokumentiert:
  - Welche Informationen erfasst werden
  - Wer sie erfasst
  - Wie sie erfasst werden
  - Warum sie erfasst werden
  - Wie man sie nutzen wird
  - Mit wem man sie teilen wird
  - Welche Auswirkungen es auf den Betroffenen haben wird
  - Ob es wahrscheinlich ist, dass die bestimmungsgemässe Verwendung zu Widersprüchen oder Beschwerden der Betroffenen führen wird.

Schützen

Einrichten von Sicherheitskontrollen, um Schwachstellen und Datenschutzverstösse zu verhindern, zu erkennen und zu beheben.

Nutzer, Daten und Geräte schützen

Sicherheit ist ein Aspekt, der in unserer computerisierteren Welt höchste Aufmerksamkeit verdient.

Zu den GDPR-Anforderungen zählen physischer Schutz, Netzwerksicherheit, Speichersicherheit, Rechnersicherheit, Identitätsmanagement, Zugriffskontrolle, Verschlüsselung und Risikobegrenzung. Sehen Sie sich genau an, wie Sie Systeme überwachen, Sicherheitsverstösse ermitteln, die Auswirkungen solcher Verstösse berechnen, auf sie reagieren und sich von ihnen erholen.

Daten

Herausforderung

Die GDPR ist nicht das Ziel, sondern der Weg. Sie verlangt von Ihnen, jederzeit rechenschaftspflichtig zu sein, bei Bedarf schnell zu reagieren und alle personenbezogenen Daten zu schützen, die Ihre Bildungseinrichtung durchlaufen.

To-Dos

- Daten und E-Mails verschlüsseln.
- Auf Geräten gespeicherte Daten (MAM) schützen.
- Sicher aufbewahren.
- Einzelne Dateien und E-Mails mit Rechten versehen.
- Einbrüche, Infektionen, Diebstähle und ungewöhnliches Verhalten beobachten und nachverfolgen.

Geräte, Standorte und Apps

Herausforderung

Geräte und Apps berühren nahezu jeden Aspekt Ihrer Daten. Ob es Teile Ihres lokalen Netzwerks (LAN), Mobilgeräte, Geräte an anderen Standorten (zu Hause oder auf dem Campus) oder Geräte und Apps in der Cloud sind – jedes Gerät und jede App bedarf der besonderen Aufmerksamkeit.

To-Dos

- Das LAN mit Antiviren- und Firewallprogrammen und physischen Vorkehrungen schützen.
- Geräte, Disketten und USB-Schlüssel verschlüsseln.
- Schüler/Studenten und Lehrkräfte über beste Praktiken im Umgang mit Heimcomputern informieren.

GDPR-Anforderungen

Die GDPR gibt Richtlinien zur Einrichtung von Sicherheitskontrollen vor, damit Schwachstellen und Datenschutzverstösse verhindert, erkannt und behoben werden können.

Nutzer

Herausforderung

Nachdem die Nutzer definiert und in Sicherheitsgruppen mit definierten Berechtigungen und Richtlinien eingeteilt worden sind, können Sie noch weitere Schutzmassnahmen – Zugriffskontrolle und Identitätsmanagement – treffen, um GDPR-Konformität sicherzustellen.

To-Dos

- Passwortrichtlinien und Anmeldeoptionen überprüfen.
- Informieren und Bewusstsein schaffen.

Testen

Herausforderung

Nachdem Sie die technischen und organisatorischen Massnahmen zum Schutz personenbezogener Daten getroffen haben, müssen Sie ihre Effektivität regelmässig testen, einschätzen und beurteilen, um sicherzustellen, dass sie sachgerecht und angemessen sind.

To-Dos

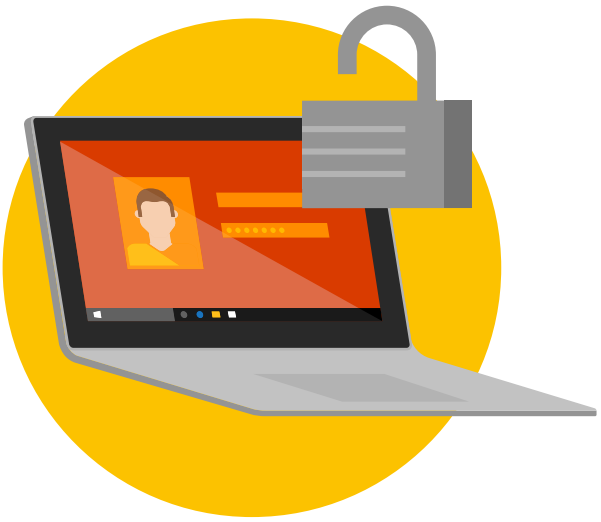
- Regelmässige Tests in die Wege leiten.
- Die Effektivität der Sicherheitsmassnahmen einschätzen.

Berichten

Auf Datenabrufe reagieren, Datenschutzverstösse melden und erforderliche Dokumentationen verwahren.

Berichten über Prüfungen und Datenschutzverstösse

Ein wesentliches Prinzip der GDPR ist die Rechenschaftspflicht. Sie werden klare Prüfpfade zur Verarbeitung und Klassifizierung und zu Dritten mit Zugriff auf personenbezogene Daten erstellen müssen, einschliesslich organisatorischer und technischer Sicherheitsmassnahmen und Datenaufbewahrungszeiten. Womöglich müssen Sie Datenschutz-Folgenabschätzungen (DPIAs) durchführen. Für eine DPIA müssen Organisationen die potenziellen Auswirkungen ermitteln und analysieren, die eine vorgeschlagene Verarbeitungsaktivität auf personenbezogene Daten haben könnte.



Prüfpfade

Herausforderung

Die GDPR verlangt von Ihnen, Verantwortung für den Schutz und die angemessene Verarbeitung von personenbezogenen Daten zu übernehmen. Ihre Datensätze müssen Angaben über jede Anfrage enthalten, die ein Betroffener macht – z. B. seine personenbezogenen Daten zu sehen oder zu berichtigen –, und darüber, welche Lösung sich dem angeschlossen hat.

To-Dos

- Speichern der Gesuche von Betroffenen, Konformität mit den GDPR-Anforderungen nachzuweisen.
- Verfolgen und aufzeichnen, wenn personenbezogene Daten in die EU hereinkommen oder die EU verlassen.
- Daten verfolgen und aufzeichnen, die an dritte Diensteanbieter (wie IT- oder Bildungsdienstleister) geschickt werden.
- Prüfpfade erfassen und sichern, um GDPR-Konformität nachweisen zu können.
- Den Strom personenbezogener Daten an dritte Diensteanbieter verfolgen und aufzeichnen.
- DPIAs ermöglichen.

Datenschutzverstösse

Herausforderung

Organisationen müssen der lokalen Behörde Datenschutzverstösse innerhalb von 72 Stunden nach ihrer Entdeckung melden.

To-Dos

- Protokolle und Berichte aktivieren.
- Innerhalb des vorgeschriebenen Zeitrahmens reagieren.
- Zur Datensicherung und Wiederherstellung im Katastrophenfall ein separates Protokoll der Änderungen an personenbezogenen Daten führen.

GDPR-Anforderungen

Organisationen müssen der lokalen Behörde Datenschutzverstösse innerhalb von 72 Stunden nach ihrer Entdeckung melden.

Schluss

Vertrauen ist zentral für Microsofts Anliegen, alle Menschen und Organisationen auf der Welt zu befähigen, noch bessere Leistungen zu erbringen. Dies ist nirgends wichtiger als in den Einrichtungen, die die nächste Generation von Schülern/Studierende darauf vorbereiten, ihre Rolle in der Gesellschaft zu finden und zu übernehmen.

Microsoft ist den Prinzipien verpflichtet, die Vertrauen in die Cloud schaffen: Sicherheit, Datenschutz, Transparenz und Compliance. Seit der Durchsetzung der GDPR in der EU am 25. Mai hat sich Microsofts breites Porftolio von Cloud-Diensten den strengen Sicherheits- und Datenschutzanforderungen unserer Kunden im Bildungsbereich angenommen und stellt sicher, dass wir Ihren Verpflichtungen als Datenverarbeiter Genüge tun.

Microsofts Cloud-Produktivitätsprodukt Office 365 A1 ist für Angehörige von Bildungsreinrichtungen kostenfrei. Es bietet die so entscheidende GDPR-Konformität sowie Informationsschutz-Werkzeuge und ermöglicht eDiscovery, Rechteverwaltung, Datenverlustverhütung, Verschlüsselung, fortschrittliche E-Mail-Archivierung und gesetzliche Aufbewahrungskapazität. Kunden, die erweiterte Risikoanalyse, Bedrohungsminimierung, Datenverschlüsselung und -kontrolle benötigen, sollten die kostenpflichtigen Pläne von Office 365 A3 oder A5 in Betracht ziehen, um ihren speziellen GDPR-Erfordernissen nachzukommen.

Kunden, die Lösungen suchen, um Datenarchivierung, Governance und Discovery für ihr breiteres IT-Umfeld zu managen, können zu Microsoft 365 Education greifen. Es bietet ihnen ein einfaches und sicheres Mittel, um Nutzer, Daten und Geräte von einem einzigen Dashboard aus zu verwalten, das Identitäten, Apps, Daten und Geräte mit intelligenter Sicherheit schützt, die durch maschinelles Lernen weiter verbessert wird.

Prüfen Sie gleich heute mit GDPR Assessment, wie gut Sie auf die neuen Regelungen vorbereitet sind. Wenn Sie bereits ein Microsoft-Cloud-Kunde sind, können Sie den Compliance Manager dazu verwenden, eine ganzheitliche Sicht über Ihren Datenschutz und Ihre Compliance-Position für Office 365, Dynamics 365 und Azure zu gewinnen.

Tools und weiterführende Links

Wir haben die nachstehende Liste von Tools zusammengestellt, um Ihnen den Weg durch die GDPR zu erleichtern.

Ermitteln

- Office 365 **Advanced eDiscovery** oder **Content Search** hilft Ihnen bei der Suche nach vorhandenen Informationen.
- **Office 365 Data Labelling** ermöglicht die Klassifizierung von Daten in Ihrer gesamten Organisation zur besseren Governance (Kontrolle).
- **SharePoint Listen** sind ein flexibles Tool zum Organisieren und Beschriften von Daten.
- **User Account Management** in Office 365 unterstützt Sie beim Organisieren der Nutzer.
- **Microsoft Intune für Bildungseinrichtungen** unterstützt Sie beim Auflisten und Verwalten vieler unterschiedlicher Geräte.
- **System Center** ist eine ideale Lösung zum Auflisten und Verwalten von Servern mit verschiedenen OSs und Cloud-gehosteten Lösungen.
- **Azure Search** erleichtert es Ihnen, anspruchsvolle Suchfunktionen in Ihre bestehende Umgebung einzufügen.
- **Azure Data Catalog** zum Registrieren, Ermitteln, Verstehen und Nutzen von Datenquellen.
- **Cloud Discovery** analysiert Ihre Datenverkehrsprotokolle unter Verwendung des Cloud App Security Cloud-App-Katalogs von über 15.000 Cloud-Apps, die nach mehr als 60 Risikofaktoren eingestuft und bepunktet sind, um Ihnen laufende Einblicke in die Cloud-Nutzung, die Schatten-IT und die Risiken der Schatten-IT für Ihre Organisation zu geben.
- **Advanced Data Governance** (ADG) hilft Ihnen bei der automatischen Identifizierung, Klassifizierung und Verwaltung personenbezogener Daten und sensibler Daten sowie bei der Implementierung von Richtlinien zur Datenaufbewahrung und -löschung.

Verwalten

- Bei Nutzung von **Security Groups** in Office 365 wird ein einziger Satz von Berechtigungen für alle Office 365 Apps festgelegt.
- **Outlook Smart Attachments** verhindert, dass Informationen über die Grenzen Ihrer Organisation hinaus verschickt werden.
- Nutzen Sie **Office 365 Mail Tips** dazu, gängige Fehler zu vermeiden.
- **Office 365 Data Loss Prevention** verhindert, dass Informationen über die Grenzen Ihres Standorts hinaus verschickt werden.
- Die Erstellung automatisierter **Flows** zwischen Anwendungen optimiert und sichert die Datenströme.
- **Intune für Bildungseinrichtungen** hilft Ihnen bei der Verwaltung von Richtlinien, Apps und Einstellungen für Ihre Geräte im Unterrichtsraum.
- **Azure AD** (Azure Active Directory) ist Microsofts Cloud-basiertes Verzeichnis und Identitätsmanagement-Service.
- Nutzen Sie **PowerApps**, um in kürzester Zeit mobile Apps zu erstellen, die Ihre Datenbanken direkt speisen.
- Beschriften Sie personenbezogene Daten mit **Labels** und managen Sie die **Data Governance** in Office 365.
- **Azure Information Protection**: Kontrollieren und schützen Sie E-Mails, Dokumente und sensible Daten, die Sie mit anderen ausserhalb Ihrer Organisation teilen.
- Das Einbetten von **Microsoft Forms** (Office 365) kann gegen Dateneinträge in Online-Formulare schützen und für GDPR-konforme Einwilligungsgesuche sorgen.
- **Office 365 Teams** ermöglicht es Bildungseinrichtungen, alle für GDPR-Richtlinien benötigten Kommunikationen .

Berichten

- Das **Microsoft Trust Center** ist eine ideale Informationsquelle über die GDPR und Compliance.
- Der Microsoft **Compliance Manager** hilft Ihnen, Risikoeinschätzungen durchzuführen; daneben vereinfacht er den Compliance-Prozess durch Empfehlung von Massnahmen, Sammlung von Nachweisen und Hilfe bei der Audit-Vorbereitung.
- **Azure Überwachung und Protokollierung** stellt Ihnen elektronische Datensätze zu verdächtigen Aktivitäten zur Verfügung und hilft Ihnen, Aktivitätsmuster zu erkennen, die auf versuchte oder erfolgreiche Netzwerkeinbrüche sowie interne Angriffe hinweisen.
- **Securescore.office.com** ist ein Sicherheitsanalyse-Tool, das Ihnen verstehen hilft, was Sie zur Reduzierung des Risikos für Ihre Daten in Office 365 getan haben, und wie Sie das Risiko weiter herabsetzen können. Es ist eine ideale Informationsquelle zur Überwachung und Protokollierung und für viele andere Sicherheitsfunktionen von Office 365.
- **Unified Audit Log** gibt Einblicke dazu, welche Daten an Dritte übertragen wurden.

Hinweis: Dies ist keine vollständige Liste der Tools und Services, die Microsoft zur Unterstützung der vier Schritte anzubieten hat. Für einen umfassenden Überblick darüber, wie Microsofts Cloud-Dienste und -Produkte Kunden bei der Einhaltung ihrer GDPR-Pflichten helfen kann, laden Sie bitte unser E-Book herunter: Schnellere Compliance mit der GDPR durch die Microsoft Cloud

Schützen

- **Office 365 (A3) Data Loss Prevention (Verhinderung von Datenverlust)** ermöglicht die Schaffung von Regeln, die verhindern, dass bestimmte Arten von Informationen nach draussen gelangen.
- **Azure Information Protection**: Kontrollieren und schützen Sie E-Mails, Dokumente und sensible Daten, die Sie mit anderen ausserhalb Ihrer Organisation teilen. Ob durch einfache Klassifizierung oder Einbettung von Beschriftungen und Berechtigungen – verbessern Sie Ihren Datenschutz mit Azure Information Protection, egal wo und was gespeichert ist, oder mit wem es geteilt wird.
- Mithilfe der **Customer Lockbox** kann der Datenverantwortliche demonstrieren, dass feste Regeln dafür bestehen, wie Supporttechniker auf Kundendaten zugreifen dürfen.
- **AppLocker** hilft Administratoren, Richtlinien zur Apps-Kontrolle aufzustellen und durchzusetzen sowie Zugriffe durch unberechtigte Nutzer zu verhindern, die personenbezogene Daten gefährden könnten.
- **Microsoft Advanced Threat Analytics (ATA)** ist eine lokale Plattform, die Sie beim Schutz Ihrer Schule/Uni vor mehreren Arten erweiterter, gezielter Cyberangriffe sowie Bedrohungen von innen unterstützt.
- **Office 365 Threat Intelligence (Daten über Bedrohungen).**
- **Intune for Education (für den Bildungsbereich)** ist eine einfache, aber leistungsstarke Lösung zum Rollout von Sicherheitsrichtlinien, Apps und Einstellungen für die Geräte in Ihren Unterrichtsräumen.
- **Windows Defender Advanced Threat Protection** ist ein mit Windows 10 Education erhältlicher Sicherheitsdienst, der es Firmenkunden ermöglicht, komplexe Bedrohungen ihrer Netzwerke zu erkennen, zu untersuchen und zu beseitigen.
- **Azure Backup** und **Azure Disaster Recovery** erhöhen die Verfügbarkeit.
- **BitLocker Drive Encryption** ist eine in das Betriebssystem integrierte Datenschutzfunktion, die Datendiebstählen oder Gefährdungen entgegenwirkt, zu denen es durch verlorene, gestohlene oder unsachgemäss ausgemusterte Computer kommen kann.
- Verwenden Sie **Multi-Faktor-Authentifizierung** in Office 365 und Windows 10 mit Windows Hello.

Dieses E-Book ist ein Kommentar zur GDPR, wie Microsoft sie zum Zeitpunkt der Veröffentlichung interpretiert. Wir haben uns lange und eingehend mit der GDPR auseinandergesetzt und glauben, dass wir ihren Sinn und ihre Absicht richtig verstanden haben. Die Anwendung der GDPR ist jedoch äusserst faktenspezifisch, und bisher sind noch nicht alle Aspekte und Interpretationen der GDPR genau definiert.

Infolgedessen wird dieses E-Book ausschliesslich zu Informationszwecken bereitgestellt. Es sollte nicht als rechtliche Beratung verstanden und nicht zur Entscheidung darüber benutzt werden, inwiefern die GDPR für Sie und Ihre Organisation Geltung hat. Wir raten Ihnen, sich mit einem qualifizierten Rechtsberater über die GDPR zu unterhalten, damit Sie ihre speziellen Auswirkungen auf Ihre Organisation verstehen und die besten Wege erkennen, wie Sie für volle Compliance sorgen können.

MICROSOFT ÜBERNIMMT KEINE AUSDRÜCKLICHEN, KONKLUDENTEN ODER GESETZLICHEN GARANTIEN IN BEZUG AUF DIE IN DIESEM E-BOOK GEGEBENEN INFORMATIONEN. Dieses eBook wird so wie es ist zur Verfügung gestellt. Die in diesen eBook enthaltenen Informationen und Meinungen, einschliesslich der URL und anderer Verweise auf Internet-Webseiten, können ohne Ankündigung geändert werden.

Dieses Dokument gibt Ihnen kein gesetzliches Recht an geistigem Eigentum von jeglichen Microsoft-Produkten. Sie dürfen dieses eBook nur zur internen Bezugnahme kopieren und verwenden.

Veröffentlicht im März 2018, Version 1.0

© 2018 Microsoft. Alle Rechte vorbehalten.